UNITED STATES DEPARTMENT OF AGRICULTURE
Farm Service Agency
Washington, DC 20250

Notice CMA-106

For: CMA’s, DMA’s, and LSA’s

Management of Sensitive (Privacy Act Protected) Data

Approved by: Acting Deputy Administrator, Management

1 Overview

A Background

For Privacy Act protected data, Notice IRM-371 provided:

- sources of authority and policy for reporting disclosures
- definitions
- restrictions on downloading and storage
- restrictions on transmissions.

All employees and contract employees, including employees of CCC approved CMA’s, DMA’s, and LSA’s, have a significant responsibility to ensure that:

- sensitive data entrusted to them is secure

- both FSA’s customer’s and employee’s sensitive personal data is not divulged to unauthorized personnel, lost, or stolen.

B Purpose

This notice:

- provides policy for managing Privacy Act protected data to help safeguard the information

- provides ACRS requirements to protect sensitive data

- reminds CMA’s, DMA’s and LSA’s of key provisions of existing Privacy Act protected data policy and clarifies what policies and actions are applicable to such companies

- obsoletes Notice CMA-105.

All FSA employees, contract employees, and partners who handle Privacy Act protected data in the performance of their duties **must** comply with this and all other applicable Federal, USDA, FSA, and OCIO ITS requirements.

Disposal Date	**Distribution**
July 1, 2008	State Offices relay to CMA’s, DMA’s, and LSA’s

1 Overview (Continued)

C Contacts

CMA's, DMA's, and LSA's shall direct questions about:

- policy to Chris Kyer by telephone at 202-720-7935.
- automation to Julie Floriani by telephone at 202-720-8374.

D Sources of Authority

The sources of authority are:

- the Privacy Act of 1974, as amended (Pub. L. 93-579, 5 U.S.C. 552a)
- 6-IRM
- Notice IRM-368
- Notice AS-2100
- the memorandum for all USDA employees and contractors from the CIO about "Protecting and Safeguarding Privacy Act Protected Information," dated June 16, 2006 (see Exhibit 1)
- USDA Cyber Security Manual Series 3500 and associated Cyber Security guidance, especially:
  - USDA Departmental Manual (DM) 3505-000, USDA Computer Incident Response Procedures Manual (March 20, 2006)
  - DM 3530-005, Encryption Security Standards (February 17, 2005)
  - DM 3550-002, Sensitive But Unclassified (SBU) Information (February 17, 2005)
- USDA Administrative Bulletin DR 3602-001, OCIO-ITS Security Policy Manual
- ITS 8000-001, Incident Reporting, Handling, and Response Security Procedures Guide
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 197, Advanced Encryption Standard.

2 Policy

A Responsibility

It is the responsibility of each individual with access to Privacy Act protected data to:

- use Privacy Act protected data in an appropriate manner
- comply with all applicable Federal laws, NIST guidance, and USDA, FSA, and ITS regulations
- safeguard Privacy Act protected data.

B Definition of Privacy Act Protected Data

Privacy Act protected data is defined as any data that contains personal identifying information including a personal name and **any** of the following:

- Social Security number
- date of birth
- home address
- financial information
- other items, collections, or groupings of information about an individual such as education (excluding training information for government employees), medical history, and criminal or employment history that contains a personal name or identifying number, symbol, or other identifying particular assigned to the individual.

While formal Government Systems of Records comprise most of the Privacy Act protected data used by FSA, any records or data that meet the above criteria can have privacy implications and should be protected accordingly.

2 Policy (Continued)

C Restrictions on Downloading and Storing Privacy Act Protected Data

Outside of a properly secured government building or approved facility without prior approval of FSA CIO, no Privacy Act protected data is to be downloaded to or stored on any of the following:

- **all** PC's, including laptops, notebooks, tablet, and those in employee's homes
- portable electronic devices, including Personal Data Assistants, text messaging devices (including Blackberries), cell phones, digital cameras, Apple iPOD's, scanners, and other mobile devices that can receive, store, or transmit data
- hard disk drives, including both internal and external hard drives
- removable media, including tapes, portable disk drives, Zip drives, Universal Serial Bus flash drives (data/memory sticks or thumb drives), smart cards, compact disks (CD-R, CD-ROM, CD-RW, etc.), DVD's (DVD-R, DVD+R, DVD-RAM, DVD-ROM, DVD-RW, DVD+RW, etc.), and diskettes ("floppy" disks).

D Restrictions on Transmitting Privacy Act Protected Data

If it is necessary to transfer any Privacy Act protected data outside of a properly secured government building or approved facility, the data needs to be protected. Privacy Act protected data (Pub. L. 93-579) **shall not** be transmitted over the Internet or e-mail systems unless encrypted through an approved method.

For CMA eligibility process submissions to KCAO according to 1-CMA, CMA's, DMA's, and LSA's already use secure FTP software to send and receive producer eligibility data.

For ACRS transmissions by cotton CMA's and LSA's to request cotton loans and LDP's, cotton CMA's and LSA's **must** begin using PKWARE according to subparagraph E.

For transmission of LSA producer 1099 data, LSA's **must** begin use of PKWARE according to subparagraph E.

For Section 1614 data sent by e-mail attachment to PSD, CMA's, DMA's, and LSA's **must** encrypt the attachment using WinZip software according to Notice IRM-372.

2 Policy (Continued)

E Reporting Disclosure or Misuse of Privacy Act Protected Data

Any accidental or deliberate disclosure or suspected misuse of Privacy Act protected data should be reported immediately to the appropriate authorities.

All users shall notify their immediate supervisor, management officials, and their local Security Liaison Representatives (SLR) if they suspect a Privacy Act protected data incident. The identity of the person reporting an incident or violation shall be kept confidential and released only on a need-to-know basis. The immediate supervisor, management officials, and local SLR shall notify the State SLR or Information Security Officer, who will follow proper computer security incident reporting procedures.

F Disciplinary Action for Deliberate Disclosure or Misuse of Privacy Act Protected Data

Any person who willfully violates Federal laws or USDA, FSA, or applicable ITS policies is subject to disciplinary action, including suspension or dismissal.

The Privacy Act states that: “Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information... and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.”

3 ACRS Requirements to Protect Sensitive Data

A General Information

To meet the requirements of the Privacy Act, CMA/LSA's will be required to:

- discontinue including producer ID numbers in ACRS transactions, except in cases where collecting the data is necessary such as the IRS Trailer Record
- submit encrypted ACRS transactions.

B Omitting Producer ID Numbers

When required by PSD, ACRS transactions for all crop years will be submitted according to 21-CN and the following:

- discontinue including producer ID numbers in all ACRS transactions except IRS Trailer Record
- fill Field 5 with zeros.

Note: CMA/LSA's will be notified by PSD of implementation date of this requirement in the near future.

C File Encryption

The National Information Technology Center (NITC) has installed PKWARE SecureZIP for z/OS, Release 9.0 that provides new security features that allow for the creation and extraction of ZIP archive files using strong 256 bit encryption. Obtain additional information on SecureZIP for z/OS at **www.pkware.com**.

All files sent from CMA/LSA's to ACRS must be encrypted using SecureZIP. Other encryption software is **not** compatible with SecureZIP.

ACRS will encrypt all files to be retrieved by the CMA/LSA using SecureZIP. The CMA/LSA may decrypt a SecureZIP file on the client side that requires 1 of the following software products:

- PKWARE SecureZIP for z/OS, Release 9.0
- ZIP Reader by PKWARE - Free Unzip and Decrypt Utility for Windows provided by PKWARE. (Replaces PKZIP 2.04G which is not compatible with SecureZIP 9.0 encryption)
- WINZIP 10. 0 and above
- PKZIP release 5.5 and above.

3 ACRS Requirements to Protect Sensitive Data (Continued)

C File Encryption (Continued)

This conversion will occur in 2 phases:

- Phase 1, when the use of SecureZIP by ACRS will be placed into production on June 22, 2007; password encryption will not be turned on at this point
- Phase 2, when all incoming and outgoing ACRS transactions must be encrypted using SecureZIP; deadline is to be determined.

D CMA/LSA Action

CMA/LSA's shall take action as follows to implement the use of SecureZIP:

- to implement Phase 1, CMA/LSA's, were instructed to unzip the test file which was transmitted June 6, 2007, and confirm that no problems were encountered

  Note: This ensured that all ACRS files encrypted with SecureZIP without a password could be opened.

- to implement Phase 2, CMA/LSA's shall provide an estimated date of when they will purchase, install, and be ready to test SecureZIP with USDA to Jan DeLancey by June 29, 2007, by either of the following:

  - e-mail to **janet.delancey@kcc.usda.gov**
  - telephone at 816-926-2638.

  Note: After estimated dates are received, an implementation timetable will be developed and each CMA/LSA will be contacted for assistance and implementation.